
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

---

## MBA PROFESSIONAL REPORT

---

# The Extent of DoD Influence on the Development and Application of Radio Frequency Identification (RFID) Technology in the Civilian Sector

---

**By:** Rafael A. Acevedo, and
Robert W. Cooper
June 2005

**Advisors:** Nicholas Dew,
Glenn R. Cook

*Approved for public release; distribution is unlimited.*

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | Form Approved OMB No. 0704-0188 |
|---|---|

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

| **1. AGENCY USE ONLY** ***(Leave blank)*** | **2. REPORT DATE** June 2005 | **3. REPORT TYPE AND DATES COVERED** MBA Professional Report |
|---|---|---|

**4. TITLE AND SUBTITLE**:
The Extent of DoD Influence on the Development and Application of Radio Frequency (RFID) Technology in the Civilian Sector

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** LCDR Rafael A. Acevedo, USN
LT Robert W. Cooper, USN

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
N/A

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release; distribution is unlimited

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** ***(maximum 200 words)***

It would be a fair argument to say that there is perhaps no invention that has had as much impact on the world as that of the Internet. The internet, however, was conceived in the minds of government employees. Just as Government influenced the development of the internet, the same can be said of Radio Frequency Identification (RFID) Technology. The DoD had a very large impact on the development of RFID. Many DoD funded projects and experiments helped pave the way for and significantly influenced the development of RFID technology. This project examines the extent of that DoD influence and shows the correlation between DoD and RFID developments in the civilian sector. From Defense projects in minefield location to tracking containers in ships on the high seas in support of the war on terror, this project explains how specific Government sponsored projects had a direct influence on the current state of RFID technology.

| **14. SUBJECT TERMS** RFID; Radio Frequency Identification; Minefield Detection; Savi; Container Tracking; Logistics | **15. NUMBER OF PAGES** 93 |
|---|---|
| | **16. PRICE CODE** |

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UL |

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

# THE EXTENT OF DOD INFLUENCE ON THE DEVELOPMENT AND APPLICATION OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY IN THE CIVILIAN SECTOR

Rafael A. Acevedo, Lieutenant Commander, United States Navy
Robert W. Cooper, Lieutenant, United States Navy

Submitted in partial fulfillment of the requirements for the degree of

**MASTER OF BUSINESS ADMINISTRATION**

from the

**NAVAL POSTGRADUATE SCHOOL**
**June 2005**

Authors: _____
Rafael A. Acevedo

_____
Robert W. Cooper

Approved by: _____
Nicholas Dew, Lead Advisor

_____
Glenn R. Cook, Support Advisor

_____
Douglas A. Brook, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

# THE EXTENT OF DOD INFLUENCE ON THE DEVELOPMENT AND APPLICATION OF RADIO FREQUENCY TECHNOLOGY (RFID) TECHNOLOGY IN THE CIVILIAN SECTOR

## ABSTRACT

It would be a fair argument to say that there is perhaps no invention that has had as much impact on the world as that of the Internet. The internet, however, was conceived in the minds of government employees. Just as Government influenced the development of the internet, the same can be said of Radio Frequency Identification (RFID) Technology. The DoD had a very large impact on the development of RFID. Many DoD funded projects and experiments helped pave the way for and significantly influenced the development of RFID technology. This project examines the extent of that DoD influence and shows the correlation between DoD and RFID developments in the civilian sector. From Defense projects in minefield location to tracking containers in ships on the high seas in support of the war on terror, this project explains how specific Government sponsored projects had a direct influence on the current state of RFID technology.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

**A. MR JERRY LANDT**

As one of the true father’s of RFID, your account of its origins, and in particular the role Government played, was extremely useful. Many Thanks.

**B. MR ROn Gilbert**

We would like to thank Mr. Ron Gilbert of Integral Technology. Your help and experience proved invaluable in our research.

**C. MR JERRY BROMENSHENK**

Thank you for taking the time to allow us to interview you. It proved most interesting and insightful.

**D. MR VIC VERMA**

Thank you for taking the time to assist us in our research. We understand you are a busy man and your time was greatly appreciated.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. THE GREAT SEAL OF AMERICA

It was 1952 and the Cold War was just starting to get heated. Neither the United States nor Russia trusted each other, a fact that that had become common knowledge. Both sides had active espionage programs well before this time and now it seems these programs were being put to some good use. What was surprising though was the lengths that the countries would go through in order to allow one side to spy on the other. In fact, when the Great Seal Bug was discovered in 1952, it had been in place for nearly a decade. (The Great Seal Bug Story)

What exactly was the Great Seal Bug? The Great Seal bug is perhaps the most publicized evidence of actual espionage between the United States and the Soviet Union (Figure 1). In 1946 a group of school children gave the United States Ambassador to Russia a gift. That gift was a replica of the Great Seal of the United States. This seal was approximately two feet across and was carved out of wood. This gift was prominently displayed in the embassy and for many years was hung in the office of the Ambassador.

What makes this story so extraordinary is that nearly ten years later during a routine sweep for eavesdropping devices, a bug was found inside the Great Seal. Why did it take ten years to find a bug in the embassy? Didn’t they conduct routine checks for such devices? Well quite simply, this bug was not your average everyday spy gadget. Most listening devices of the day were passive but were

either on or off. They had to be manually operated and were generally planted in the on – or constant – listening mode. This made them fairly easy to detect during normal sweeps.

**Figure 1. Replica of the Great Wooden Seal Presented to Ambassador Harriman. (After:NSA)**

The signal was detected and all was well. The great Seal bug, however, remained passive until it was activated by an external signal transmitted from outside the embassy. In this manner, it could be turned on or off at will by the Soviet Government. This meant that traditional detection devices were none the wiser to its existence. This was essentially a remote controlled covert listening device developed in 1946 (Figure 2). While it can be argued that the Great Seal device was not a true instance of RFID

because it didn't actually identify anything, the similarities with respect to the technology are startling.[1]


**Figure 2. May 26, 1960. Ambassador Henry Cabot Lodge, Jr. displays the Great Seal bug at the United Nations. (From: NSA)**

## B. WHAT IS RFID?

In layman's terms, Radio Frequency Identification (RFID) is the process of uniquely identifying an object using radio waves. There are two major components to an RFID system; tags and readers. And while the size, shape, and type of tags and readers vary with the manufacturer, the basic premise behind the operation of any RFID system remains the same. A tag is first placed in or on an object. In the case of The Great Seal bug, the tag was embedded in the gift. This object can be anything from a case of beer to a family pet to a shipping container. Electronic tag readers are then placed in specific

[1]Although the device was found in 1952, it was not until 1960 that the world learned about its existence. The information had been withheld due to the political climate of the time. (The Great Seal Bug Story)

locations that will allow them to be able to receive the information – or identification – being sent by the tag. There are essentially three main categories of tags: active, semi-active, and passive.

**1. Active Tags**

The first type of tag is the active tag. Active tags actually have a transmitter built directly into the tag itself. This transmitter runs off of a battery that is also in the tag. The tag sends a signal to a reader that may be hundreds of feet away. Because of the fact that this tag has its own power source, it carries the longest ranges of all the categories of tags. In fact, because the tags are transmitting, readers placed at extended ranges can be connected to a satellite communications network which allow that data to then be received just about anywhere. (Gilbert, 2005) This is particularly useful when you are looking at shipping container data. The benefit being that a shipper would know where the goods were at all times, and the receiver would know whether or not the container had been opened or altered in shipment.

Active tags have their downsides, however. Due to the fact that they contain a battery and transmitter, they are several times more expensive than their passive tag counterparts. A SaviTag, for example, is $105.00. (Savi Website, 2005) If you only need a handful of tags, this may be no problem. However if you are talking about a corporation in need of several thousand tags, the use of active tags would be cost prohibitive. The startup cost would be too much for all but the largest companies. Additionally, the addition of these items also necessitates

a tag size that is much larger than passive tags. In fact, they are roughly the size of a cigarette pack. This means that they cannot be used in anything requiring a miniature tag such as animal tagging.

**2. Semi-Active Tags**

Semi-Active tags incorporate some of the benefits, and also some of the disadvantages, of both active and passive tags. Semi-Active tags do not have a transmitter, but they do contain a battery. The fact that they have a battery inside the tag itself means they can be read at greater ranges than passive tags but less than those of active tags. Why? Because the semiconductor in the tag is powered by the battery in the tag so it doesn’t have to be powered by the energy in the radio waves from the reader. The benefit of this is an extended range of roughly 100 feet or so. (Gilbert, 2005) Again, because these tags have a battery they are both more expensive and larger in size than passive tags, giving them some of the limitations as active tags. Semi-Active tags are roughly the size of a pack of gum.

**3. Passive Tags**

The last category of RFID tag, and perhaps most common, is the passive tag. Passive tags do nothing until they receive a signal from the reader. In fact they can’t really do anything else because they have no internal power. They derive their source of power from the signal the reader sends. They then use this power to send a signal back to the reader. Because they have no internal power supply, they do not have the ability to amplify the signal being sent by the reader. This means that the

ranges are reduced, averaging less than 10 meters. While lack of a battery is a disadvantage, it allows for two of the greatest advantages of these types of tags – size and cost. Passive tags are small – very small, measured in inches or millimeters depending on the tag. The chip itself can be made as small as a grain of sand. (Gilbert, 2005) This means that the tags can be used in a variety of places where a large, obtrusive tag is prohibitive. These potential uses include but are not limited to animal and human tagging. In theory, any object could be tagged.

## C. RESEARCH QUESTIONS

### 1. Did Governmental Influence Impact the Development of RFID Technology?

The development of the internet is perhaps the most publicized success story of Governmental influence on the development a technology. The internet has touched the lives of nearly every person on this planet. Even people in developing nations who don't have computers or internet access are impacted by the World Wide Web from other nations who are bringing aid and supplies. What is important to realize, is that without Governmental interest in developing technologies we wouldn't even have the internet. Can the same be said about RFID? To what extent did a confluence of Governmental interest and programs influence the development and application of RFID?

### 2. In What Ways Has the Development of RFID Technology Impacted the Civilian Sector?

Did Governmental influence on the development of RFID technology affect the civilian sector? If the answer is "To some extent, yes," then in what ways did it affect that sector? What are some of the specific mechanisms through

which this influence occurred? In this paper, we trace these influences through a historical analysis of DoD programs and initiatives.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. METHODOLOGY

## A. THE SEARCH

Initially we set out to try and discover just what information was available on the development of RFID. We knew through various sources that RFID was a hot topic. After all, with the Wal-Mart and DoD announcement requiring the use of EPC tags, the subject was very newsworthy. An EPC, or Electronic Product Code, is a unique product identifier for a particular good. An EPC is similar to a UPC except that a UPC requires manual scanning while an EPC contains an RFID chip that allows for automatic reading of the tag. It was our opinion, that the first step in determining whether or not the Government had indeed influenced the development of RFID had to be an investigation into the historical origins of the technology. When did the topic of RFID first come about? Did it piggy back with other technologies? Who was responsible for introducing the technology as we know it? These were all questions we knew we had to answer if we were going to get a feeling for what role, if any, DoD had played. And subsequently, if it did play a role, exactly how much impact did it really have on the development of the technology?

Thus began the exhaustive search to determine the true origins of RFID. We began with an internet search to see what information was quickly available. What we found was that there is no shortage of articles relating to the development of this technology. In fact, there were numerous pieces written on the subject of RFID. Perhaps

the two best sources were Jim Eagleson's RFID: The Early Years 1980-1990 and Jerry Landt's Shrouds of Time. These documents provided the most comprehensive look we had found to date on the development of the technology. That said, they did leave gaps in the timelines that we had a hard time resolving. What we needed was more details.

**B. INTERVIEWS AND SPECIFICS**

By conducting the previously mentioned comprehensive search for existing data, or literature review, we had a rough idea for the genesis of RFID technology. We knew for example that the development of radar and IFF was a major stepping stone. Additionally, work had been done regarding RFID in Los Alamos, yet the precise nature of the work, or the extent that it may have impacted RFID development were still not known. These were huge gaps that had to be filled in order to say with any degree of certainty that the DoD or Government had been the major presence in its development. The problem was that after all the information available had been analyzed, there were significant holes in the thread of RFID history. There was plenty of data and information on current civilian RFID projects. Wal-Mart and EPCs; Savi and container tagging; Transcore and the transportation industry; tons of privacy issues; and numerous medical use experiments. However, none of these went back early enough to provide a good picture of how it all began, which of course is what this project hinged on. There was not one succinct article that explained the history of RFID and its emergence as a technology today in the detail required. What was the spark so to speak that ignited the development of RFID as we know it and did the Government provide that spark. So

the decision was made to start from scratch and get the information straight from the horse's mouth(s).

We decided to talk to those people who had been in the field of RFID development long enough, and had enough expertise to hopefully give some thread or lead with which to spin this web of the history of RFID. This is really where the first big break came. After pouring through countless sources with information on RFID (most of which said the same thing and were not very helpful) we noticed a trend. A great many of these sources kept mentioning the same names over and over. Mr. Jerry Landt and Mr. Ron Gilbert were consistently mentioned in several RFID related documents. The best place to try and add some continuity to all of the information that had been collected was to speak to these gentlemen first.

Ron Gilbert was working at Alien Technology just up the road here in central California. We drove up and interviewed him in person. The information and leads that arose from this interview were an enabler to future research. Ron had worked at Los Alamos early on during the development of RFID technology and had some interesting insights into the development of the technology.

The next gentleman interviewed was Jerry Landt. The interview was conducted via teleconference. Mr. Landt has a very extensive background in RFID. What made him so unique as a source of information is that he was there at what can be argued was the beginning of this development. As we discuss later in this project, Los Alamos is arguably where most of the backscatter RFID technology as we know it began. Backscatter is similar to radar in that a signal is

sent towards an object. It then bounces off that object and some bit of this signal is scattered back and received by a reader. Jerry holds several patents and his knowledge of early RFID achievements. Interviewing Jerry, however, led to some interesting thoughts.

First was the seemingly rapid nature of development after the first known Governmental contracts were let to Los Alamos. With ARPAnet, the Government played with it a while and it took some time to develop into a functioning technology outside of the DoD. That was not apparently the case with RFID technology. Government contracts seem to be the catalyst for civilian sector development of RFID, but it was surprising just how quick the move was from Government program to civilian innovation – less than a decade.

Secondly, it became very apparent through our interview and later somewhat confirmed by what we found independently, that RFID technology was still in its infancy. In fact, prior to the 1970's, there had been little actual forward progress in the arena of RFID. Although Harry Stockman can be said to intimate the beginnings of this technology in 1948, RFID technology was essentially stalled for nearly 30 years. (Landt, pg. 4) It appears that Stockman was right when he wrote:

> Evidently, considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored. (Landt, pg. 4)

Lastly, our interview with Vic Verma at Savi provided us with a wealth of knowledge into Savi's and the

Department of Defense's development of cargo container tracking technology. His experience at Savi and his enthusiasm during our interview allowed us to answer several questions that had eluded us. In turn, we were able to discern the telltale signs of an emergent path dependency to RFID.

## C. PATH DEPENDENCY

What is path dependency? Put simply, path dependency is the outcome of a technology based on past technological outcomes rather than on current technologies.

### 1. The Case of QWERTY

Probably the most famous example of a path dependent technology is that of the common computer keyboard interface, otherwise known as the QWERTY keyboard. The QWERTY keyboard was invented in 1874 by Christopher Sholes when he introduced the first "modern" typewriter. The keyboard arrangement was is response to a design flaw in the initial typewriter to prevent jamming of the type bars in the machine.

In his original design, the keyboard was laid out in a more alphabetical layout, but repeated quick type strokes would cause jamming between the type bars, which needed to be unjammed. The results of his experiments led to the development of the QWERTY layout as it spread the most used keys across the entire keyboard. This layout was accepted by E. Remington and Sons who then proceeded to market the first typewriter. As competitors entered the market, the QWERTY layout was already established with typewriter users, therefore, Remington's competitors would use the layout as well. This practice has continued to this day

even though much more efficient models of keyboard layouts exist. (Diamond, The Curse of Qwerty)

### 2. RFID and Path Dependency

So what does the QWERTY keyboard layout and RFID technology have to do with one another and how are they related? As stated above, QWERTY has come to dominate the world of the computer keyboard industry simply by being the first layout to be used by consumers and therefore becoming the most widely known. RFID has already made a significant impact on a global scale and is being adopted by more users everyday. Is that to say that RFID is a bad thing? Not at all. In fact, RFID Technology is proving to be a valuable asset in supply chain visibility.

So how has path dependency affected the development of RFID? During Operation Desert Storm, the Department of Defense realized a need for better asset tracking in its supply chain. With this need in mind, it turned to the civilian sector to solve this problem. Savi technology was awarded several grants in the early 1990's to develop an efficient tracking system for DoD assets. Savi in turn, improved upon existing RFID technology in the marketplace to create a truly transparent supply chain. This technology has been readily adopted by the US Army and is beginning to see more acceptances across the other services. It is in the civilian sector where path dependency and RFID are truly apparent.

As RFIDs use continued to rise within the DoD, the DoD began to encourage the use of RFID with all of its suppliers; however, it would not be until Wal-Mart mandated to use of RFID from its suppliers that the world began to take notice. Shortly thereafter, the DoD mandated its use

as well. With the world's largest retailer and the United States department of Defense both demanding RFID Technology, the global marketplace has rushed to adopt this technology.

**3. Creating a World Standard**

But what of the technology itself? RFID is now considered a vital asset in the tracking of supply chains. But what is the standard? Will RFID become like the mp3 player market, where it is dominated by one player and several smaller competitors? Apparently, no. With the adoption of Savi's 433Mhz technology as an open standard, ISO 18000-7, this specific RFID technology can now be used by all companies interested in supply chain logistics.

> I want this company (Savi) to be a small fish in a big pond vice a large fish in a small pond. (Verma, 2005)

**4. "Open" Standards**

Savi's RFID technology is now an open standard. Its use is becoming ubiquitous across the entire Global Marketplace. With this acceptance, RFID is now growing to meet the demands of the world economy. Just as path dependency dictated the adoption of the QWERTY keyboard, so too has RFID become the de facto standard in supply chain logistics.

But, conversely with QWERTY, RFID being an Open standard lends itself to constant improvement. A good example of this is the MACINTOSH and WINDOWS/DOS debate. Although Macs were technically superior in all forms to its Windows competitor, when it was first introduced, the Mac was not backwards compatible with the previous Apple II line. This caused immediate problems with its consumer

base and as a result allowed Windows to take over the market with its backwards compatibility with previous DOS programs. (Verma, 2005)

Being an open standard, Savi's RFID will be constantly improving, both with technical innovations and market competition. And even though the infrastructure for RFID is being built worldwide, that infrastructure lends itself to upgrades as well, and therefore avoids stagnation, which would eventually create serious problems in the worldwide supply chain.

There is no doubt that RFID has become a path dependent technology. Through Dod's support and adoption of Savi's standard, the DoD, now with the largest integrated total visibility network, has caused other manufacturers to adopt the same technology as well in order to take advantage of the network already developed by DoD. This in turn creates more users and will eventually lead to a worldwide standard originally based on the technology funded by the DoD.

# III. BIG BROTHER

## A. NECESSITY IS THE MOTHER OF INVENTION

### 1. RADAR is Born

September 1, 1939. The world watches in horror as Germany invades Poland. World War II has officially begun. For the citizens of Great Britain, the war has been brought right to their doorstep as France and Britain declare war on Germany on September 3, 1939. (MDEP.org, 2004) The one bit of good news is that the new invention called the RADAR for Radio Detection and Ranging has been greatly improved upon since its original inception around 1922. (Landt, 2001) Radar was a dramatic improvement in the art of modern warfare. It capitalizes on the principal of reflected energy waves in order to detect an object at great distances. Radio waves are transmitted out and then the energy reflected off of an object is returned back. By using the difference between the time the radio waves were transmitted and the time the waves return, the radar is able to calculate the distance. The radar knows what direction it sent the waves so the bearing is also available. This data provides the range and bearing, or location, of an object from the radar site. For the first time in any conflict of our age, one side could see the enemy approaching before the enemies weapons could reach them.

### 2. Identify Friend or Foe

Radar proved to be a most useful technology. Shore installations and ships could now tell how many aircraft were in the sky and where they were located. What radar could not solve, however, was the problem of

identification. With so many Allied and German aircraft in the sky at any one time, it could get very confusing for the radar operator. Visual identification and sight was required on all targets in order to confirm whether they were enemy or not. This had two results. The first result was that many friendly pilots were killed due to fratricide because they were mistaken for enemy fighters. The second ill effect was that because the gunners were worried about shooting down friendly planes, they had to wait until the Germans were right upon them to get a positive enemy identification. By then, they had lost the tactical advantage and the German fighters often got the upper hand.

The answer was a system still in use today (although somewhat more advanced than the original version) as Identify Friend or Foe, or IFF as it is more commonly known. IFF was likely the earliest application of RFID as we know it in that it used a transponder on the aircraft that stayed passive until it was hit with a signal, or radio wave, from the radar system that was "interrogating" it. Once the transponder on the friendly aircraft received the signal it responded with a signal of increased amplitude. In other words, the signal sent back to the radar was bigger than that it had sent out, thus identifying an aircraft as friendly.[2]

## B. RFID – BOMBS TO COWS

### 1. Los Alamos

On July 16, 1945 the first nuclear weapon in history was detonated at Los Alamos, New Mexico. (Weideman, 2004)

[2] www.vectorsite.net The use of IFF continues today and is still in use in civilian and military aircraft around the globe. The systems are more advanced, but the RFID technology inherent within them remains. (14 April 2005)

Los Alamos National Laboratories had been set up in secrecy during World War II to develop the A-Bomb developed the first practical RFID technology thirty years later.

Not only had the atomic bomb been invented at Los Alamos, but in the years that followed World War II the site continued to develop and test these weapons. New innovations such as using Hydrogen to fuel the weapon along with miniaturization to make the weapon fit in a missile as opposed to a very large bomb were all being developed at Los Alamos. (LANL website) The best and the brightest of the scientific community were still resident at the New Mexico facility for much of this time, making it a perfect breeding ground for developing technology. This changed, somewhat, in 1963 with the passing of the Limited Test Ban Treaty. This treaty required underground vice above ground testing. (LANL website) A confluence of some of the most intelligent minds in America, a secure facility, a climate of innovation, and a shift in focus after the Limited Test Ban Treaty were all factors that made Los Alamos ripe for the development of new technologies. And while the concept of RFID technology was not new, the practical development and application of the technology had not yet been realized. The chance to make this technology work came from a grant from the Department of Agriculture, and Los Alamos filled the bill.(Landt, 2005)

**2. Cows**

The problem with cows is that the dairy business is very labor intensive. In order for the animals to produce milk, they need a specific diet that must be heavily monitored. Hence the need for RFID tags. The idea was to tag the animals with an RFID device. This would allow the

farmer to not only identify and keep track of the animals, but also to relay back information such as body temperature. The potential benefits of this were enormous. If the system worked, it promised to give the farmer an in-depth look into the cows physical condition, it would aid the veterinarian in their diagnosis, and it would ensure that the cow was mated at the appropriate time. All of which promised increased efficiency which meant dollars to the farmer, and potential reduction in costs to the end consumer. It is also important to note that this technology was not just being researched and developed in America. Europe, Holland in particular, was very interested in animal tagging. (Landt, 2005)

**C. TECHNOLOGY TRANSFER**

The work at Los Alamos continued for several years, and although many developments were made with respect to the specific designs of the tag, it was not until the mid 80's when things really started to take off. What caused the spark? Well the answer is the confluence of several things. By the 1980's there were many pieces of the puzzle in place to give RFID a fighting chance. There was a significant interest in tagging both animals and other items from the civilian sector as well as other foreign governments and there was also a series of complimentary technologies that aided in development. As Jerry Landt put it - "the transistor, the integrated circuit, the microprocessor, development of communication networks, changes in ways of doing business." (Landt, 2001) were all needed in order to truly jump start the development of the RFID technology. The 1980's gave the technology just such a start.

Here in the United States, the foray into RFID which begun at Los Alamos would take on a new life when two private corporations, Amtech and Identronix, were formed as a result of a technology transfer between the government and the civilian sector initiated in 1977. (Landt) This allowed the companies to take technology developed under government contract and use it to advance their own research in the area of RFID. This was crucial move as it provided the civilian sector with more creative freedom to develop the technology that American Industry was interested in.[3] Amtech was later bought by Transcore, who continues to be a world leader in ground transportation solutions through the use of RFID technology.

**D. GOVERNMENT AND INDUSTRY COLLABORATE**

By the mid 1990's, RFID technology was booming. It was being touted (and still is in many circles) as the answer to many identification-related problems. One issue in particular garnered interest by both Government and Industry alike. That issue was trademark infringement and the counterfeiting of clothing goods. Both the textile industry and the Department of Agriculture were facing a big problem with respect to theft of trademarked good through illegal sale and manufacture. Counterfeit goods made overseas and imported into the United States were sold at much cheaper prices and were nearly indistinguishable from the real thing. The problem wasn't how to stop the items from getting in the country, but rather how to protect the consumer. When you buy a Rolex watch for 20

[3] American Industry was not particularly interested in tagging animals. Rather, tagging vehicles (trains) and other items turned out to be of greater value to many businesses. (Landt, 2005)

dollars from the man on a New York Street corner, you accept some risk that the watch you are buying is not actually a Rolex. The problem comes when you buy an item from a reputable store who just happens to be the victim of a supplier who provided counterfeit goods. RFID looked to be the perfect answer. So in 1995, the American Textile Association teamed up with Pacific Northwest National Labs and began to investigate a solution. (Gilbert, 2005)

The idea was to see if there was a way to meld RFID into the product tag of a pair of Levi's™ jeans or a designer shirt such as Nautica™ or Hilfiger™. The tag could solve two problems at once. First it could allow for better control and a more accurate inventory of the product for both suppliers and retailers. Secondly, and perhaps most importantly, the presence of the tag would enable the retailers to know that they received an authentic item. Because counterfeit good would not contain this tag, telling them apart would be a snap. Consumers could then feel safe in their purchases of these goods from retailers who were using this technology. (Gilbert, 2005) The technology, however, was not yet advanced enough to allow this to be cost effective. The individual cost of the tags in 1995, combined with the readers, and associated hardware would make this option too expensive. Additionally, for the first time, dealing with consumer goods, privacy issues started to arise. Would the tag "turn off" after it was purchase? Could it transmit information about its wearer such as location? Could the consumer's information be collected and stored in a database that could potentially be unsecured? While these are not necessarily problems of technology, they are social engineering issues that would

have to be dealt with before implementation of this technology could become a reality.[4]

**E. TRACKING DR. STRANGELOVE**

Once again Los Alamos was in the picture as the birthplace of the first Atomic Bomb would also prove to become the birthplace of the technology destined to keep those self-same nuclear weapons, and their related components, safe. In 1975 the Department of Energy awarded a grant to Los Alamos National Laboratories to study and develop ways to maintain constant supervision of nuclear weapons. The Department of Energy was concerned over the long distances of rail lines that nuclear materials sometimes traveled and desired a way to maintain constant tabs on whatever materials or devices were being shipped.

Los Alamos labs realized that a technology was being developed that could meet several users needs at once. The cow tagging technology of RFID could also be used to protect nuclear materials. The nuclear safeguards project was born. The goal of the Project was to develop an active RFID device that would be able to be interrogated at a distance and it be able to respond back in answer to the interrogation. This would prove to be difficult as the related technologies such as circuit boards and computer processor chips were just beginning to make their own evolutionary leap. It would not be until the very late 80's and into the nineties that true miniaturization would occur. (Landt, 2005)

Lasting until 1982, the nuclear safeguards project resulted in the development of vehicular mounted RFID

[4] AMTEX information was provided by Mr. Ron Gilbert formerly of Alien Technology. Ron is now the Chief Technical Officer for Integral RFID.

devices that not only were able to identify the automobile they were in, but were also capable of detecting if any nuclear material was in the automobile itself. The devices themselves were very large, approximately the size of a brick. This technology actually proved to be too sensitive as some personnel who were known to work with nuclear materials found themselves and their cars searched due to false alarms due to the sensitivity of those devices. The project proved to be successful. Even though the size of those RFID devices were colossal compared to the devices of today, the nuclear safeguards project at Los Alamos National Laboratories would lay the ground work for future uses of the technology in the transportation industry.

## F. THE CIVILIAN SECTOR AND RFID

### 1. Speed Pass

Beginning in the 1990's, RFID saw an explosion in the use of the technology in the civilian sector. Companies such Exxon-Mobile Corporation introduced their speed pass card for their customers in order to make a customer's time at the pump more convenient. Using an encrypted low frequency (LF) RFID signal, the speed pass card is able to communicate with a base transceiver located in the gas pump via an encrypted signal. Proximity is required for this transaction due to the fact that this is a passive process. When the speed pass is "swiped" in front of the transceiver, the customer's personal information is downloaded and the appropriate credit card that the consumer has chosen is billed.

While it is true that active tags would provide a greater range, their cost and size would make them prohibitively expensive and impractical for the individual

consumer. In fact, as of 2004, gas companies are experimenting with fully automated gas stations. These gas stations, upon a customers arrival at the pump, reads an RFID signal from the automobile, asks the customer what grade of gasoline and how much they would prefer, automatically fills the car and charges the customer's credit card. (Discovery Channel, 2004)

**2. No More Toll Lines**

Gas Companies were not the only ones to benefit from this technology. State and Local governments would also begin to deploy this technology for their own benefit. Toll roads are a much-needed generator of funds for the state. The tools help maintain roads and equipment used to maintain those roads as well as other important government functions. However, many drivers simply avoid them due to the congestion that can occur at highway tollbooths. By adding RFID technology to the tollbooths and the automobiles passing by them, a means was now available for the state to maintain its money flow while not inconveniencing the drivers.

This first occurred in 1991 as Oklahoma opened the world's first electronic tolling system. This system was designed so that drivers could maintain the speed limit. When they passed a RFID interrogator, the system would determine if the car had been tolled yet. If the car had not, the owner's appropriate credit card would be charged; all while not affecting the driver at all. Video surveillance cameras at the toll collection points were put in place in order to prevent people from taking advantage of the system. If a car passed the collection point and no acknowledgement was received, the video camera would

activate to get a picture of the offending automobile's license plate and subsequently alert the authorities. This technology was quickly adopted across the country. In 1992, Houston, TX installed the world's first toll and traffic information system and Kansas installed a system that not only read the RFID signatures of its customers, but the customers of Oklahoma's system as well.[5]

**G. THE GOVERNMENT'S CONTINUING SUPPORT**

The United States government would continue to support the development of this technology throughout the 1990's with grants and contracts. The Department of Defense would become a very large proponent of RFID technology as it was recovering from the massive logistical nightmare that was Operation Desert Storm.

As DoD's support for RFID continued throughout the 1990's and early 2000's, it set forth a standard in 2003 making mandatory the use of the Electronic Product Code standard. This was done shortly after Wal-Mart instituted the same standard for its operations. With the largest defense agency and the largest retailer in the world now demanding the use of the same standard, RFID (EPC) became the standard protocol for all defense contractors and supply chain providers for Wal-Mart.

Although these standards are now mandatory, the government is continuing to fund further research into the continuing development of RFID technology. As of March 2005, the United States Government has awarded three additional contracts to civilian companies to continue the development of this evolving technology, particularly in

[5] The Shrouds of Time

the area of logistics tracking and EPC tag and reader development. (Army Contract Website)

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. THE DEPARTMENT OF DEFENSE AND SAVI TECHNOLOGY: CREATION OF A WORLD LEADER

## A. HISTORICAL BACKGROUND

### 1. The Gulf War

August 2nd, 1990. Saddam Hussein's Iraqi Military invaded Kuwait under the cover of night. Saddam claimed rights to the territory of Kuwait under old Ottoman Empire borders. He also claimed that Kuwait had cost Iraq nearly $14 Billion in oil revenues from theft of oil in the Iraqi oil fields of Rumaila.

The United Nations called for the immediate withdrawal of Iraqi troops, and when that failed, enforced an immediate embargo of all goods going to and from Iraq. US Forces in Saudi Arabia moved to protect the Saudi Oil fields. A coalition was formed of several nations and the largest buildup of American troops since the Vietnam War began.

In total, nearly a half million troops were assembled to drive Saddam's forces from Iraq. Saddam refused to heed the United Nations ultimatum of a Jan. 15 withdrawal from Kuwait and on Jan 18th, Operation Desert Storm was launched.

Thirty days of sustained air attacks followed by four days of ground operations pounded the Iraqi positions. On Feb 28th, President George H. W. Bush declared a cease-fire as most of the Iraqi forces in Kuwait had surrendered, been destroyed, or fled. This is the story that popular history tells of the First Gulf War. What it doesn't tell is the massive logistical problem the Coalition was faced with as

it attempted to maintain the fighting capability of the troops on the ground and in the air.

**2. Money Down the Drain**

Nearly forty thousand containers from hundreds of different suppliers, contractors, vendors, and the Department of Defense itself found themselves placed in the massive supply depots in Saudi Arabia. All told, nearly 6.5 million tons of equipment was shipped to the desert of Saudi Arabia. Of those forty thousand containers sent, over half were opened to determine their contents the moment they arrived in theater. This was a time and manpower intensive job as inspectors were forced to empty and repack container after container in search of the parts that they required. The other half, a number estimated to be around twenty-five thousand, were never opened and left in the "Iron Mountains" of containers that stacked up outside the ports. This lack of control of the supply system caused commanders to order the same parts several times which resulted in $2.7 billion dollars of parts going unused and sitting in the Arabian desert for months and sometimes years after Operation Desert Storm. (Davis, p. 229)

> Had AIT (Automatic Identification Technology) solutions been implemented at the time of Operation Desert Storm, it would have saved the Department of Defense over $2 billion in logistics and supply chain costs - GAO Report (Wykle, presentation)

Fast forward fifteen years and this is what is now said about Department of Defense Logistics.

> This command believes RFID offers the best potential for immediate in-transit visibility and

> should become the joint operational standard for all services. USCENTCOM will require all air pallets, containers, and commercial sustainment moving to/from the theater and intra-theater movements to be tagged with RFID at origin for asset and in transit visibility tracking in the CJOA. - General Tommy Franks, USCENTCOM (Wykle, presentation)
>
> The most successful radio frequency and tracking implementation in the world is the US Department of Defense. - Craig Harmon (Wykle, presentation)
>
> The technology solutions for DoD parts tracking and inventory has an annualized payback of $24 million. - Coopers and Lybrand study on DoD Parts Tracking (Wykle, presentation)

## B. THE CREATION OF AN INDUSTRY STANDARD

### 1. The SaviTag

How did the Department of Defense become the world leader in the implementation of Radio Frequency Identification Technology (RFID)? The answer begins in 1989 when a man by the name of Rob Reis lost his two-year old son after he wandered off in a grocery store. Thankfully, he found his son, but at that moment, he came up with the idea of a "tag-a-long" system that would be able to track small children. He founded Savi Technology in 1989. (Savi Technology Website)

In 1990, The Defense Advanced Research Projects Agency (DARPA) awarded Savi an initial contract to explore and develop technologies for the tracking of goods in supply-chains. Savi then began to transition from child tracking technology to supply chain technology and in 1991 was awarded three Small Business Innovation Research (SBIR) grants from the US Navy amounting to $2.5 million dollars.

These funds, including those from private investment, allow for Savi to develop the SaviTag.

> Savi Technology, Inc. of Mountain View, California recently developed the industry's first radio computer tag, the "SaviTag," using a combination of Navy SBIR funding and private venture capital. The SaviTag, a radio transceiver with an embedded microcomputer, can be attached to military cargo containers - or any other crate or container used for transport - and will automatically track the container's location and contents. The SaviTag was developed with just $2.5 million in SBIR Funding (three awards) and has become a central element in DoD's Total Asset Visibility effort - the DoD effort to be able to pinpoint the location and content of every plane, ship, tank, and cargo container in transit around the world. - Testimony of Daniel Hill, Assistant Administrator for Technology, US Small Business Administration (Hill, p.3)

The SaviTag was first used in 1993 and 1994 as ammunition retrograde was being returned from Saudi Arabia. This retrograde material was marked and tagged with an RFID tag and shipped to military installations in Europe. The result was a marked increase in the reliability and accuracy of the shipments and their manifests. The SaviTag

ST-410 would become the de Facto standard for the US Army's RFID logistics program during the 1990's.

**Figure 3. SaviTag (After: Raytheon)**

### 2. Developing a Standard

Due to continued humanitarian operations throughout the 1990s, including Somalia, Haiti, and Bosnia, the US Army would become the largest user of RFID technology until the creation of USCENTCOM and its directives for the entire service community. Using the new technology, the US Army noted a 30% reduction in logistics assets for operations in Somalia and later, in the Bosnian theater.

At this same time, in 1992, The DoD initiated its first Total Asset Visibility plan. The TAV was defined as "the capability to provide timely and accurate information on the location, movement, status, and identity of units, personnel, equipment, and supplies." (DoD, 1992) The TAV plan set forth the objective for all of the services including the US Coast Guard, to begin to implement RFID technology in its respective supply organizations and the vendors and contractors that work with that service.

This was a preliminary plan, the implementation of the plan would not occur until 1995, and the standards for DoD

RFID requirements would not be finalized until 2003 under a memo from the Undersecretary of Defense for Acquisition, Technology and Logistics. In fact, the individual services would not even be mandated to use RFID until 2002.

In 1994, Savi was awarded its first major DoD contract totaling $70 million dollars and would become the first and primary supplier of RFID Tags to the US Military. The purpose of the contract was to provide hardware, software, and the infrastructure required to build and manage a worldwide RFID network.

In 1995, the DoD TAV implementation plan was published creating the Joint TAV Office, which would be in charge of the implementation and operation of the TAV plan across all services. At this same time the US Army was the largest user of RFID technology and owned the majority of all RFID assets in the DoD. It assumed the role as executive agent of RFID technology to the DoD.

In 1997, Savi was awarded its second DoD Contract totaling $111 million dollars for continued support of the TAV plan for the DoD. The infrastructure that Savi continues to build leads to the DoD's ITV (In-Transit Visibility) network. The DoD's ITV network would become the largest active RFID-enabled cargo tracking system in the world with over 800 tracking stations in 45 countries.

April 29th, 2002. The Strategic Council on Security Technology is formed with Savi Technology as a founding member. Its goal is to provide for the development and implementation of technology that can ensure the security and integrity of the world's supply chains. In order to meet this goal, the SCST drafted the Smart and Secures Tradelanes initiative. After the events of September 11th,

2001, it was deemed that the security of containers and other means of cargo storage and shipment were woefully under protected and that the security of the business that housed these cargo containers as well as the ports and cities that held them were vulnerable to terrorist attack. The SST initiative set forth a policy dictating the securing off all cargo containers at their point of origin using special RFID tags that once sealed could not be reopened without damaging the tag and therefore alerting the authorities.

Another important aspect to the SST initiative is that not only is one of the world's leaders in RFID technology (Savi), a member, but three of the world's largest port authorities. In fact, combined, these three port authorities represent nearly seventy-five percent of the world's trade. Although still in its infancy, container tagging, monitoring, and shipment are becoming a major security issue not only in the United States, but the world in general. With the threat of weapons of mass destruction falling into the hands of terrorists, container security is becoming an issue on the forefront of National defense.

In 2003, Savi was again awarded the primary contract for RFID support for the DoD totaling $90 million. In addition to the US Department of Defense, Savi was also awarded contracts for RFID supplier for Great Britain's Ministry of Defence and the ministry of Defense for Denmark. It was also awarded the contract to provide RFID technology for a NATO pilot program to determine if Savi's RFID technology can be used enhance NATO's, and its 19 member countries, logistic collaboration. This is in part because of a US DoD offer to share its existing ITV network

for joint operations. After a long evaluation, NATO chose to use the same technology as both the US and the UK. The pilot program would establish a network of integrated supply chains from the Netherlands and Germany through Uzbekistan and finally to NATO Headquarters in Kabul, Afghanistan.

> Savi's contract with NATO is a major first step in bridging supply chain information gaps to ensure that the right vital supplies get to the right place at the right time,' said Bruce Jacquemard, Savi's Executive Vice President and General Manager for Global Field Operations. 'This is a proven, battle-tested solution during times of conflict and peace that will bring new levels of consignment visibility and collaboration to NATO allies, whether for internal tracking purposes or joint force operations. (Savi Technology, 2004)

## C. TOTAL ASSET VISIBILITY

### 1. National Defense and Matryoshka Dolls

DoD's use of RFID technology has increased significantly since Operations Desert Storm. During Operation Iraqi Freedom, US and UK supplies numbered between fifty and sixty thousand pallets and containers. Each one of these was tracked using active RFID. In fact, there were more than five hundred RFID nodes that could monitor and edit active RFID data in the theater of operations. Now it is estimated that DoD's RFID network now monitors over 270,000 cargo containers across the globe. (Davis, p.231)

How does the DoD, and Savi, maintain this massive network and keep tabs on the incredible amount of supplies that are being transported across the planet? In October of 2003, the Undersecretary of Defense for Acquisition

Technology and Logistics issued a policy directing the approach as to how the DoD would use and develop its RFID network. The memo was in five parts and consisted of the following:

- Directed the continued use of active RFID tags in support of ongoing operations
- Required DoD suppliers to put passive RFID tags on the lowest individual part or package by January 2005.
- Directed all DoD component commands create a capability to read passive RFID tags at key installations by January of 2005.
- Created a DoD RFID Integrated Product Team. The IPT was given five goals to achieve:
- Suggests to DoD components that they should begin to plan to include RFID in their budgets, as the DoD would not provide any additional funding. (Davis, p232)

The memo also identified six layers of the DoD supply chain where it expected to implement these new RFID standards.

- Layer 5: The transport by which the cargo is moved.
- Layer 4: The cargo container or pallet in which the supplies are held.
- Layer 3: Warehouse pallets, unit loaded supplies, or fiberboard packaging.
- Layer 2: the unit carton
- Layer 1: Bubble wrapped supplies
- Layer 0: The individual item (Davis, p232)

A Russian Matryoshka Doll is an excellent example of how this technology and "nesting" of RFID components to track the DoD supply chain occurs. The Matryoshka doll is made up of several increasingly smaller dolls that are carved to fit exactly inside the doll that is one size larger than itself. When placed inside, the smaller doll is encased by the larger doll, which is then placed inside another larger doll eventually forming one complete doll.

**Figure 4. Typical Russian Matryoshka Doll (After: RussianCrafts)**

Just as the dolls nest inside one another, the DoD system builds its supply network using the six levels. Beginning with the individual unit, is tagged and programmed with a passive RFID tag. That unit is then placed with other units and wrapped. The wrapped package is then tagged and programmed with another

passive RFID tag to represent all of the individual tags contained within. Proceeding up the chain, all of the wrapped packages are then stored together in a container, which then again, is tagged with another passive tag. These containers are then collected and placed within a single 20ft or 40ft Cargo container or a standard DoD pallet. That container or pallet is then given an active RFID tag that is programmed to transmit the entirety of its contents when interrogated. These cargo containers or pallets are then placed on their subsequent transports for shipment. This entire process ensures that every single item that is shipped is accounted for. Examples of hardware can be found in Figures 5-7

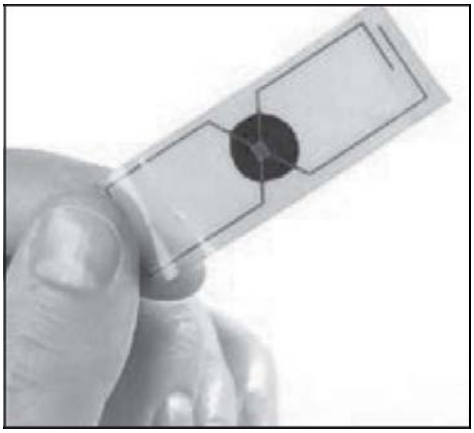


**Figure 5. Passive RFID Tag (From: AFLMA)**

For instance, the port of Antwerp, the largest port in the world, has already built a comprehensive active RFID network. This allows the port to monitor all of the containers within the port's premises to ensure not only the proper handling of containers with perishables, but to also maintain the security of those containers. This Total

Asset visibility is continually improving as new technologies are introduced.


**Figure 6. Portable RFID reader and active RFID tag (From: AFLMA)**

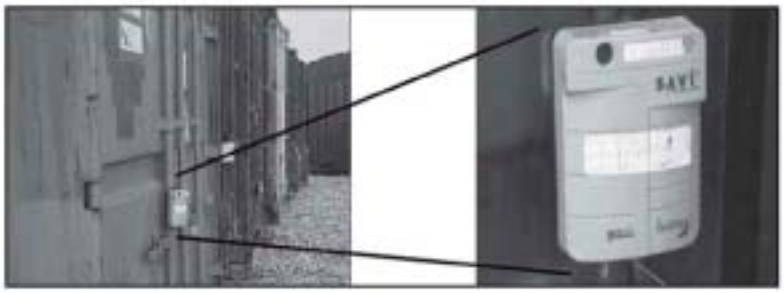



**Figure 7. Active Savi container tag copy (From: AFLMA)**

First introduced in October of 2003, the Savi Sentinel ST-646 is a new form of active RFID tag that actively monitors the container that it is assigned. The Sentinel is placed door of a container and is designed to detect any tampering with the seals on that container. The Sentinel can also monitor interior conditions of the cargo container by monitoring tags within the container itself. The Sentinel can monitor for changes in environmental conditions such as temperature, light, shock, vibration, atmospheric pressure, chemicals and even radiation from inputs it queries from the passive tags located in the container itself. (Savi Technology, 2005)

For example, the DoD now uses this type of technology in order to monitor MREs (Meals Ready to Eat) while they are in transit to ensure they do not spoil. The Sentinel lends itself well to Savi's commitment to the Smart and Secure Tradelanes initiative. However, it is but one link on the chain to provide better security for supplies, not only on a producer to customer basis, but for national security as well.

This Active-Passive relationship leads back to what was discussed earlier in the Methodology chapter. The technology, although constantly evolving, always moves back to the initial line of development between the DoD and Savi. This path dependency based upon the initial funding of the DoD, will influence the development of this Technology for years to come.

In 2004, Savi announced the development of RFID-ACT (Assured Compliance Today). This technology allows for vendors and contractors to meet the technology requirements of the DoD. By taking advantage of its position as Primary DoD supplier, Savi was able to develop, with partners Zebra and Symbol Technologies, a means for businesses to comply with the new standards set forth by the DoD in 2002. The standards are based on the EPC 856 format that Savi helped develop in the 1990's. (Savi Technology, 2005)

**2. Savi's International Acceptance**

In 2003, the International Organization for Standardization (ISO), adopted the RFID standard ISO 18000-7, which covers the use of RFID in the 433 MHz range. This range, of course, is the standard set by Savi in the Nineties when it was developing the DoD's ITV network.

In April of 2004, and later that summer in June, both the United States Federal Communications Commission (FCC) and China's State Radio Regulatory Commission (SRRC) both gave their support for the 433Mhz radio-frequency band which is used by Savi's worldwide network for its active RFID tags and security seals.

> These back-to-back decisions by the world’s largest manufacturing center (Peoples Republic of China) and largest consuming nation (U.S.) provide further momentum in the adoption of a global active RFID standard, which is critical for seamless visibility of cross-border, international shipments,” said Fraser Jennings, Savi’s vice president of Standards and Regulatory Activities, who has been active in proceedings with both the FCC and SRRC. “A common global standard for active RFID has been needed for a long time to ensure total asset visibility across all links in the supply chain. We’re increasingly encouraged that the 434 MHz band is rapidly gaining acceptance as the official standard for real-time visibility across the entire supply chain worldwide.(Savi Technology, 2004)

Will Savi's 433mhz standard become the global standard? Only time will tell. However, it should be noted that Savi is approaching this possible worldwide acceptance with a certain humility. Savi is driving for this technology to become an open standard, therefore allowing its competitors to use and even improve upon Savi's technology. Like the QWERTY keyboard, this path dependent technology will no doubt remain for years to come, but unlike the QWERTY keyboard, this technology is built to be improved upon.

Since 1991, Savi Technology has been on the forefront of technology in the field of RFID. From a modest company of one person when it was founded in 1989, Savi has grown into a worldwide leader in RFID Technology. Starting from a small grant from DARPA and later the Small Business Administration, Savi would be able to develop the technology needed by the Department of Defense and win a major military contract only three years later. From then on, Savi would go to develop the world's largest In-Transit Visibility Network and gain contracts from not only the US Department of Defense, buy the United Kingdom's and Denmark's Ministries of Defense and NATO. Savi's contribution to the civilian sector cannot be overlooked. Savi involvement in the Smart and Secure Tradelanes initiative involves it with the world's largest cargo carriers and port authorities. This partnership will lead the way to develop more secure supply chains around the world and will help to provide an additional layer of security for the United States Homeland Defense.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. THE HONEYBEE STORY

## A. BACKGROUND

### 1. The Korean Crisis

The year is 2007 and North Korea's nuclear rhetoric has reached a boiling point. After repeated demands by the world's leaders for the country to give up its nuclear weapons program, North Korea has yet to accede. The United Nations is preparing to issue the fourth in a series resolutions designed to get the rogue nation to acquiesce to global sentiment requiring the immediate cessation of a nuclear weapons enrichment and development program. Additionally the United States has indicated that this will be the final resolution. There will be no more diplomatic measures participated in by the United States to resolve the North Korean nuclear crisis. The deadline has been set. The President, in an address to the nation, made the following statement:

> My fellow Americans, I come before you tonight to speak about a growing evil in our world. This is an evil that represents an immediate and grave danger to the security of the United States and the lives of every American. I am of course referring to North Korea's growing arsenal of nuclear weapons and ever-advancing delivery methods.
>
> Since 2003 when North Korea recommenced their nuclear weapons program, the United States has made every effort to achieve a diplomatic solution in an attempt to get North Korea to cease any further development of nuclear weapons. These efforts, I am sad to say, have been fruitless with North Korea continuing to advance its nuclear weapons program in an attempt to

> extort the world into meeting its never ending list of unreasonable demands.
>
> The continuation of a nuclear program by a nation so openly hostile to the United States and freedom is unacceptable. North Korea currently possesses a limited number of nuclear weapons and in a short time will have the capability to deliver those weapons to the Western coast of the United States. We cannot stand by and wait until they achieve this capability. I have therefore ordered the deployment of U.S. forces to the region and should North Korea fail to comply with the latest United Nations call for nuclear disarmament, the United States will take action to disarm them.

Nine months later the United States has amassed its forces in the region and with North Korea's steadfast refusal to comply, hostilities are imminent. The North Koreans are confident. They know that an amphibious landing in the North by United States forces will be extremely difficult. They rapidly changing tides and rocky shore make a suitable attack from the sea an unattractive option. The North Koreans have correctly surmised that the primary means of attack by United States and South Korean soldiers will be straight across the border at the 38$^{th}$ parallel. This is great news for the North Koreans because they have been heavily mining the border for decades. It is nearly impossibly for troops of either side to safely make it through. Although the North Koreans were the ones who initially laid the mines, they have long since lost track of the exact whereabouts of each individual mine, making transit through the area extremely dangerous.

What the North Koreans don't know, however, is that the United States Special Forces have been along the border

for months. They have been conducting surveillance and mine mapping operations. In addition, they have been actively disarming mines at a rapid pace and the United States forces now have a lane several miles across with which to safely enter North Korea once the hostilities begin. So how did our forces achieve what many have called an insurmountable task similar to finding multiple needles in a barn full of hay? How could the North Koreans have been wrong? After all, they had all but declared the border impassable due to the presence of such a large number of mines.

### 2. Tactical Honeybee Unexploded Ordnance Detection System (T.H.U.D.)

What the North Koreans didn't know, and in fact much of our own military and civilian leadership did not know, was that the United States has been developing a secret weapon. In fact, since the late 1990's, the Defense Department has been funneling money into a top secret project whose primary goal has been advanced rapid and accurate mine detection and classification. The **T**actical **H**oneybee **U**nexploded Ordnance **D**etection system, or T.H.U.D, became fully operational last year. The system uses honeybees to sniff out mines and then relays locating data back to a central command post through the use of radio frequency identification tags. These tags are attached to the backs of the honeybee, allowing the command center to track the individual bee as it marks the mine. Then, using the Global Positioning System, or GPS, and the data received from the tags on the bees, computer software creates a three dimensional map of the minefield. The

result is perhaps the most accurate and error free mine detection system ever devised.

The scenario given above is obviously false. That said, the premise behind such a scenario occurring is very real. Should a situation such as that of North Korea come to fruition, the United States lacks an efficient and credible mine detection and classification system. While the development of a system involving the use of honeybees to detect, locate, and classify mines is not quite as advanced as the story made it out to be, it is nonetheless a very real program currently under development.

## B. BEE BIOLOGY

Could bees actually accomplish this? Well there are actually a number of reasons for choosing bees for the program, and yes, all evidence indicates that bees are indeed a very viable method of detection. The first reason for choosing bees is that they have a very acute sense of smell. In fact, their ability to detect smells rivals that of dogs that are notorious for their ability to track a scent. Both dogs and bees can detect scents and vapors down to parts per trillion (pptr). “Like dogs, bees can detect suites of chemicals, such as 2.4-DNT, 2.6-DNT, TNT, and RDX over a wide range of concentrations.” (Bromenshenk, 2003) Wouldn’t it be much easier to just train a dog? It has to be easier than training a bunch of bees. The bees have a couple of advantages that dogs don’t. First of all, a dog has to walk through the mine field to detect the mine. Bees, however, do not have to roam the same ground the mines are in. They do not need to physically touch the ground. This means that they can detect the mine without setting it off.(Bromenshenk et al, 2003) A dog also

requires a handler to go with it. When people use dogs to find things, they have them on a leash. This is to ensure that the dog does not just take off and decide there is a steak somewhere else that it would rather be looking for. Bees do not require a leash because they will almost always return to their hives. (Bromenshenk et al, 2003)

## C. FACT OR SCIENCE FICTION?

### 1. The Government Sponsored Bee Hive

So we have answered the question of "why bees?", but we have yet to answer the question of can it work. Can they really do this? Or is this notion of a bee detection system purely hypothetical science fiction? Well it just so happens that that is exactly what Dr. Jerry Bromenshenk, a Professor at the University of Montana, set out to prove under a three year project funded by the Defense Advanced Research Projects Agency's (DARPA) Controlled Biological and Biomimetic Systems Program. DARPA began funding research into the development of a mine and unexploded ordnance detection and classification system using common honeybees as the method of detection in the late 1990's. The idea was to see if these insects could indeed be used for the aforementioned purpose. Specifically, could these bees differentiate between a field with mines embedded throughout and ordinary land that did not contain mines? Additionally, if this project was to be successful, the bees would have to be able to detect individual mines, or at least individual clusters of mines. Without these critical abilities, the project would not be viable. It is, after all, inherent in a mine detection system that the system actually be able to correctly detect and identify specific mine locations.

**2. The Results are In**

The answer came in the summer of 2003 when Dr. Bromenshenk's team at the University of Montana, in conjunction with Sandia National Laboratory, S&K Electronics, Air Force National Laboratory, and the National Oceanic and Atmospheric Administration's (NOAA) Environmental Technology Laboratory successfully conducted field trials at Fort Leonard Wood in Missouri. The results were phenomenal. Specifically, the bees accomplished all of their objectives with some surprising results. To begin with, the bees were successfully tracked at hundreds of meters. (Bromenshenk, 2003) This is crucial because minefields can be very wide. The ability to track individual bees over a particular target mine is a must. Secondly, the bees were able to differentiate between mines and mine clusters and they homed in on the majority of the required vapors. (Bromenshenk, 2003) What this translates into is accuracy and validity. Both of which are essential for effective mine localization. The resulting map generated from the bees' results is depicted in Figure 1. (Bromenshenk, 2003) As you can see from the image, the ability to locate mines and generate a visual depiction of their location utilizing honeybees as the detecting source is a very real and viable concept. One unexpected result that was obtained through this field trial was the validation of the ability of the bees to differentiate between affected and non-affected areas. That is, their ability to tell a minefield apart from a normal un-mined area. This was not immediately evident from the trials as the bees homed in on a specific area of the non-mined test location. This would, at first glance, seem to indicate

that the bees were confused and that this particular test objective was a failure. Upon further investigation, it was discovered that the location in the un-mined test area that the bees had homed in on, actually did contain trace amounts of explosive residue. In reality, instead of being wrong, the bees detected explosives in an area where none was believed to exist. The practical applications of a mine detection system this accurate are staggering. Imagine not just the military uses, but the humanitarian utility of such a system. Between 2001 and 2002 over 74 countries were actively engaged in some kind of mine clearance operation.[6] In most cases, the mines are being found through the time consuming use of metal detectors. Think of the time, effort, and lives that could be saved with a system like T.H.U.D.

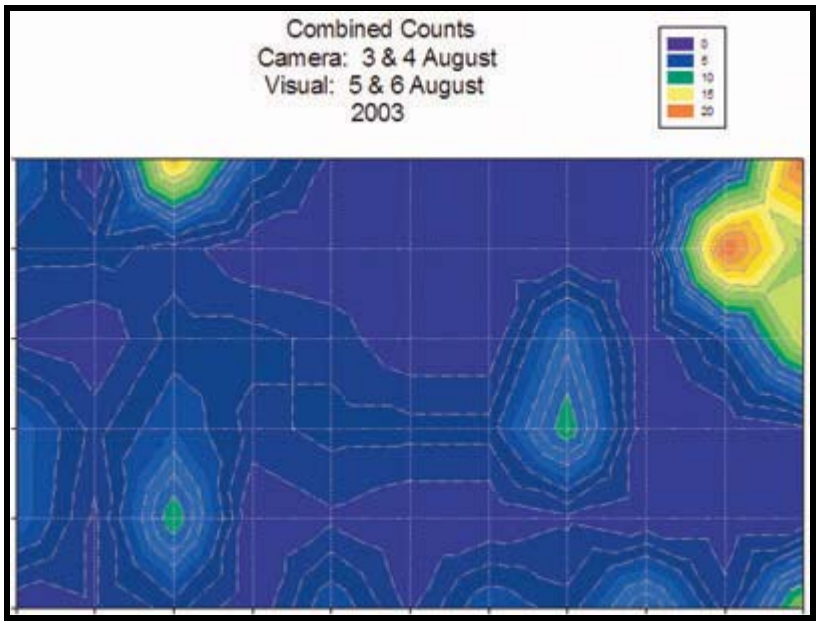



**Figure 8. Bee-generated map of a minefield. (From: Bromenshank)**

[6] Mine monitor report, 2002

## D. BEES GET STUNG BY RFID TECHNOLOGY

### 1. Size Does Matter

So we know the system is feasible and some would even say probable. But what does any of this have to do with RFID? The answer is actually pretty simple. Bees can find land mines fine, but how do you find the bees? That is, how do you know precisely where they are? If a bee travels over a mine and detects explosives, that positional data needs to be somehow retransmitted back to a central location for collation and mapping. Additionally, the position needs to be precise, and you to know which bee went where. RFID could be the key to getting the right data where it needs to be to make the system effective. When Dr. Bromenshenk's team initially began working on the DARPA project, they looked to RFID to help solve the problem of locating all of the bees. We are talking about thousands of bees and multiple hives, with each bee requiring its own tag. Additionally, the capabilities of RFID tags meant that much more data could be transmitted back than just position. Metrics such as hive temperature, air temperature, and humidity could all be given as well. Putting an RFID tag on a bee would also, however, require that the tags used be extremely small. The first tag they tried was designed by Pacific National Laboratories and weighed in at 28mg. This tag was much too big for a bee to successfully fly with. A second tag, designed by Tim Schaefer of the Mayo Institute developed a smaller tag that was a mere 10mg. The team thought that they finally had a workable tag. So much so that many publications raved about the how successful the use of RFID would prove to be in locating landmines now that the problem of size had been

solved. The reality was, however, that once the actually field trials had begun it quickly became evident that the tag would not work. While it was small enough to fit on a bees back, it impacted the bee's flight and hindered the project. (Bromenshenk, 2005)

The problem was not simply the size of the tag. The tag had to be small enough to ensure it did not impact the bee's natural behavior and flight, however, the size of the tag itself represented only one of the issues associated with putting RFID tags on bees. The second major issue stemmed from the fact that although the size of the tags had been decreasing through evolution and breakthroughs in the processing technology, the size of the antenna was still much too large to be used on a bee. Just for a little review, remember that in order to achieve the smallest possible size in the tag, it must be passive. That is, it does not have a battery with which to boost the signal back to the reader. This means that the antenna has to be of sufficient length to generate the appropriate ranges required for practical mine locating operations. Although there were antennas that were sufficiently small enough for this application, there was no method for connecting them to the small tag and then affixing them to the bee – super glue was just not going to work. Unfortunately for Jerry Bromenshenk and his team the technology did not yet exist that would allow for an antenna that small to be attached to a tag that small and then inserted onto a similarly small insect. That is until the evolution of Direct Writing.

**2. Direct Writing Fills the Gap**

"'Direct Writing' technologies are used to produce, or

deposit materials on, complex two or three-dimensional structures." (DTI, 2005) In short, Direct Writing is a manufacturing process that allows for the placement of almost any two or three dimensional object, of nearly any size, onto another object. What's more, is that the kinds of materials capable of being produced and/or deposited on is almost limitless. Glass and metal, alloys, crystals, ceramics and synthetic materials (e.g. plastics) and natural organic materials including biological are all kinds of materials this technology could be used for. (DTI, 2005) The potential for inclusion of this new technology into the RFID/honeybee equation was immense. While this technology has been around for several years, it wasn't until 2002 that Doug Chrisey at the Naval Research Lab demonstrated the ability to affix a foil antenna to the back of a bee (Figure 2) using a laser direct-write technique (Figure 3).

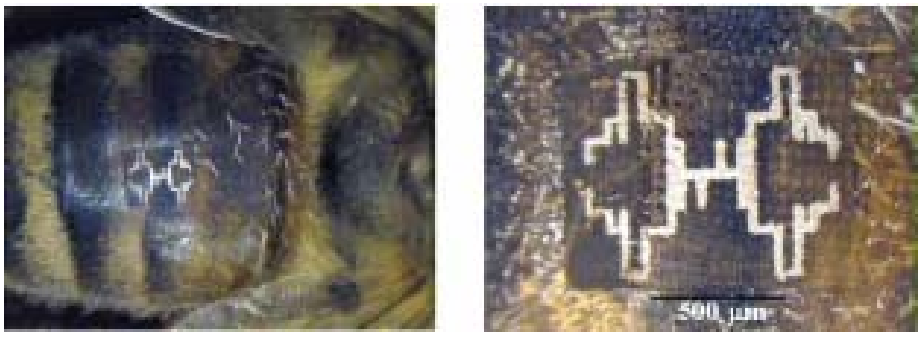


**Figure 9. A fractal antenna written on the back of an adult honeybee.[7](From:Chrisey)**

[7] Future of Direct Writing. Doug Chrissey et al write up regarding future of direct writing technology. This leads to the notion that this technology is just getting to the point where it might benefit RFID development.

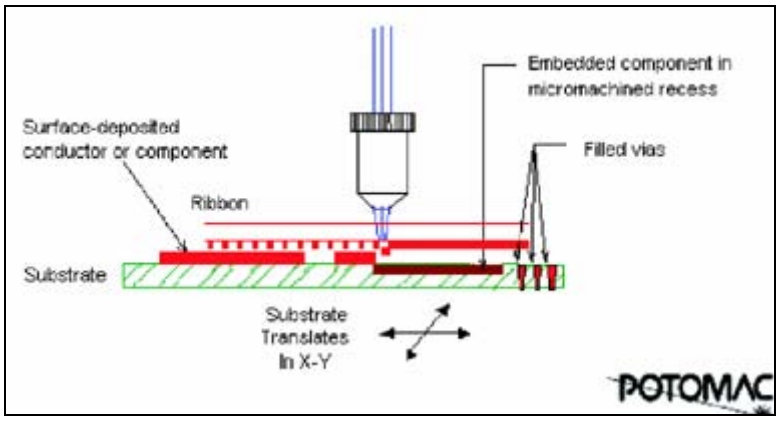



**Figure 10. Illustration of Laser Direct-Write Technique (From:Advanced Micro-Electronics)**

This meant that it was now technically feasible to use an RFID tag to track a honeybee conducting mine hunting operations. Unfortunately, the DARPA contract ended in 2002. Jerry and his team decided to continue moving forward on their own, but abandoned the notion of using RFID to track the bees. The technology was just not mature enough to make it a viable option. While it had been shown that an antenna could be fixed to the back of a bee, an antenna/tag combo had not yet been attempted. Additionally, there was no guarantee it would work. There were also fiscal concerns. Because RFID was still relatively in its infancy in 2002, as far as technology maturation is concerned, the cost of an RFID tag made the use of the tags cost prohibitive and impractical. We are, after all, talking about thousands of bees; each bee with its own tag costing nearly five dollars a piece. Do the math, it was just too expensive. So the team decided to use LIDAR (Light Detection and Ranging). (Bromenshenk, 2003) LIDAR is similar to RADAR (Radio Detection and Ranging). In fact, a version of it is used by police

officers all over the country to enforce speed laws. It uses laser light reflections to measure distance. Laser light signals are sent out where they contact a target, in this case the bee, and then are received at a reader to control center. The time between the signal that was sent and the signal that was received is compared to get the distance of the bee. (Wikipedia, 2005)

But is the LIDAR system good enough to track at the individual bee level? Absolutely! In fact, by tuning the LIDAR to the frequency of the bee's wings, the system is able to filter out all non-bee contacts..

**E. WHAT'S NEXT?**

So what's now for the future of bees, mine hunting and RFID? Well, officially, the project involving the use of bees for mine detection has completed and the use of honeybees to explore minefields is no longer on the table. There have been, however, tremendous strides in the last couple of years in the development of RFID tags and reader technology. The cost has come down significantly. In fact, tags are now as low as 20 cents depending on the quantity sold. The uses for RFID in other bee applications are also wide and varied. For example, in the state of Montana alone, there are over 200,000 bees at over 6000 different locations. (Bromenshenk, 2005) And while it may not make the evening news, bee hive theft is a major issue for beekeepers and honey producers. One sure fire way to ensure that the bees don't get stolen is to insert an RFID tag into the hive. Passive tags would help the owner to find their hive by letting them know when they got close. Active tags, on the other hand, while more expensive, could potentially send back signals giving the exact location of

the bee hive – many states away if necessary. Additionally, as previously mentioned, the use of RFID tags has another added benefit. With today's tags that hold even more information, the tag can relay important data with respect to the current conditions at any given time within the hive. This could save beekeepers a great deal of time from having to take the readings themselves.

Jerry Bromenshenk and his fellow researchers hold several key patents with respect to the use and conditioning of bees to detect airborne chemicals such as explosives. They have formed a company called Bee Alert Technology which is based out of Montana and continues to research uses for bees and their training methodology. Why do we care about that? We care because the use of bees and RFID in Department of Defense applications is far from over. In fact the Army's Small Business Innovation Research Program just gave the green light to commence Phase II of project topic A03-160: Honey Bee Fast Response System for Broad Band Detection of Airborne Toxicants. (ARO, 2005) And who do you think got the contract – that's right, Bee Alert Technology. The same group of people that worked on the original project that began over 5 years ago. This project, in similar fashion to the mine detection project, has the team training the bees to detect and locate other airborne toxins. These could include anything from mustard gas to anthrax. I think it safe to say that at least for the immediate future, the concept of using bees to locate and identify airborne chemicals will be a hot topic. And don't think that RFID is out of the picture either. Dr. Bromenshenk and his team at Bee Alert Technology have been working with Chris Parkinson and Ron

Gilbert of Integral RFID to develop a small, cost efficient RFID solution for the tagging of the bees. As originally conceived in the DARPA mine project, the use of RFID is back on the table. (Bromenshenk, 2005)

The honey bee mine detection story is a perfect example of how technology maturation is dependent on a multitude of factors. Specifically, the reason it can take decades from the birth of a technologically advanced idea to the development of its practical applications is because the evolutionary ladder of technology must be built. That is, the new advancement is at the bottom of the ladder and it is not until each of the rungs has been developed and put into place that the technology can go up the ladder and reach maturation. An example of RFID technology maturation in the context of honey bee applications is shown below in Figure 4.

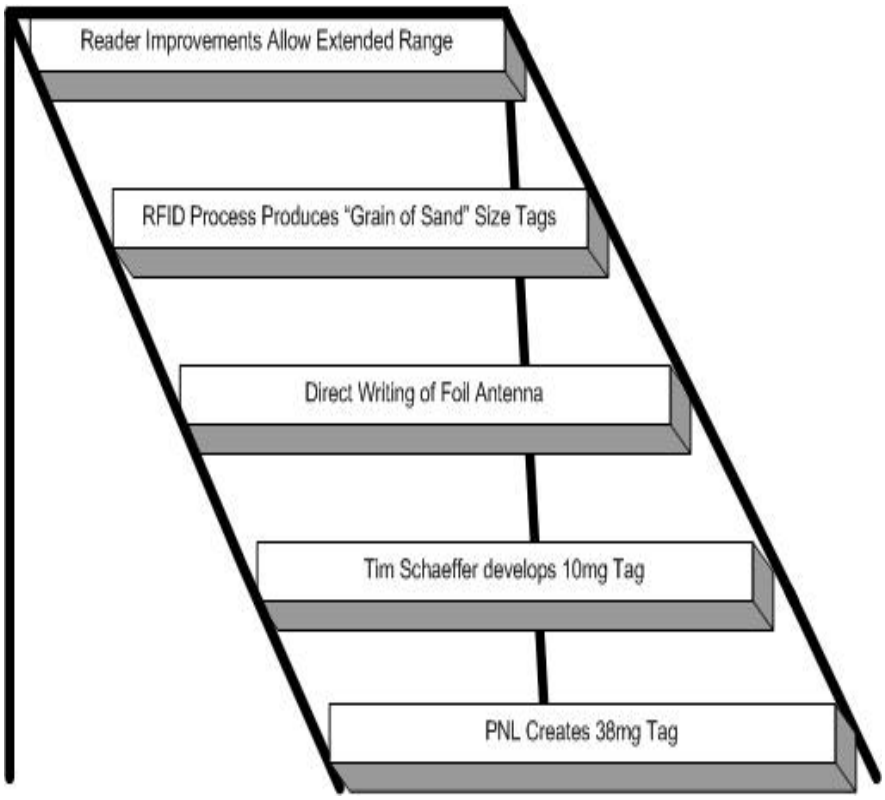



**Figure 11. Honeybee/RFID Technology Development Ladder**

THIS PAGE INTENTIONALLY LEFT BLANK

# VI. CONCLUSION

## A. FOUNDATIONS

RFID technology has made significant strides since it was first developed in the 1970s at Los Alamos National Labs. Beginning as a modest effort into monitoring livestock as part of a grant from the Department of Agriculture, RFID as we know it in the 21st century has evolved into a wide-ranging technology that affects the United States and the rest of the world every day. Shortly after the grant from the Department of Agriculture, the Department of Energy saw in RFID a reliable means of tracking and safeguarding nuclear material as it was transported across the country. As both of these technologies began to take shape, it became readily apparent to its creators that the amount of applications that RFID technology could be applied to was virtually endless.

RFID has not just made its presence known in the fields of supply chain management, but also in more esoteric forms. The honeybee project, as described earlier in this report, is a perfect example of the adaptability of this technology as it jumps from corporate monitoring to becoming a tool for the military. It should be readily apparent that the United States Government, specifically, the Department of Defense, not only funded RFID development, but has lead the way to general acceptance of this technology.

But even before the Department of Defense became involved in the technology, the Department of Agriculture and the Department of Energy would lay the groundwork for

the first working prototypes; specifically, the DARPA and SBIR grants to Savi, which in government terms were rather insignificant, have lead to contracts in the hundreds of millions of dollars. Rather impressive for a company that was founded by one man trying to develop technology to track a wayward child.

Now in the 21st century, only thirty years after the first RFID chip and receiver were created, it now permeates society. It has undergone transformation into the premier method of supply chain visibility both within the United States Government as well as the civilian sector. It has transformed transportation in several parts of the world, offering fast, convenient access to toll roads and eliminating tollbooths. It has created a world leader in RFID technology, Savi technology, who has itself helped transform the security of cargo containers in shipments around the world. Even though the DoD has only just now mandated the use of RFID for all services, RFID has still seen significant use as Savi now manages the DoD's ITV network. This ITV is now the largest in the world.

## B. SUSPICION AND DISTRUST

Due to RFID's relatively new birth in the global market, it has been met with suspicion as a way to track individuals covertly. While that capability is entirely possible, the political implications for the use of RFID are more important. During Operation Enduring Freedom, Many containers containing RFID tags and receivers were turned away at several countries borders because the local customs agents believed that they were espionage devices of some sort. This led to delays in deliveries of needed supplies to the troops on the ground. For RFID technology

to truly expand on a global scale, Government as well as business must take steps to demonstrate to their trading partners that RFID, when used responsibly, can help reduce costs and in the long run, improve efficiency as well as the security of their own countries.

## C. IDEA, CONCEPT, REALITY

The role of the Federal Government in the development of RFID Technology cannot be denied. Looking back to the 1970's, the major grants by the departments of Agriculture and Energy started the proverbial wheels turning on this emerging technology. It is interesting to follow the development of RFID as time continued. As if the government had planted a seed, RFID was now growing and branching into other fields.

From the Department of Agriculture grants came, of course, the cow tagging technology. This technology laid the groundwork for further development in the fields of remote biometrics. The technology would then branch into the American textile industry in the 1980's as clothing makers were looking for ways to defeat counterfeiters. Copies of famous name brands were beginning to appear in the third world black market and manufacturers were concerned that this would adversely affect the perceived quality of their goods. This would then lead to further developments into miniaturization of RFID tags, as they would be placed into articles of clothing in order to verify the authenticity of the designer clothing. (Landt, 2005) This eventually would branch into retail security and general goods tracking across the supply chain.

Just as RFID branched in one direction it also developed from methods created from the Nuclear Safeguards

Project funded initially by the Department of Energy. The technology built into this program would eventually migrate to into the public transportation field, as all trains in the US would be marked with RFID, although each car was outfitted with two passive tags vice an active tag used in the Nuclear Safeguards Project; which actually, would make this an amalgam of the technologies developed both for nuclear safeguards and the initial cow-tagging program. This technology would also be adopted by the gas companies as seen in the development of Speed pass technology. This technology would also lead to the development in toll road technology that now permeates the United States as well as Europe.

**D. WHAT DOES THE FUTURE HOLD?**

Wal-Mart, the world's leading retailer, announced in 2005 that it expects its top 100 suppliers to be EPC (electronic product code) compliant by 2006. Being the leading retailer, Wal-Mart's new policy has sent shockwaves throughout the manufacturing industry as businesses rush to meet this new requirement. This announcement also came on the heels of the Department of Defense's announcement that it also wanted full compliance for its vendors and contractors. With the both the world's largest defense agency and the world's largest retailer both requiring this new technology, the business world stood up and took notice. In fact, Gillette Corporation, a major supplier to Wal-Mart, recently ordered 500 million RFID tags from Alien Technology. While not admitting that this was in reaction to Wal-Mart's new policy, it comes after Wal-Mart's announcement. Such a large scale purchase from a major corporation in order to meet the demands of another large

corporation will no doubt force business as a whole to take a closer look at this relatively new emerging technology.

The Department of Defense has already begun to take steps in its ITV network to be able to incorporate Generation II RFID tags as they become available. As the size of RFID tags decrease, their future uses can only be guessed. Some scientists look toward using them to track blood flow through a person's bloodstream. This could help to determine circulation throughout a person's body. The tagging of pets is already a reality, is the tagging of children on the horizon? With recent high profile child abduction cases in the news, Public outcry for child safety is reaching an all time high. Will this open another door for RFID? It is interesting to note that Savi Technology's initial charter was the development of technology to track children. Will Savi, or one of its competitors, brave public opinion and enter this field? Only time will tell.

RFID has taken the world by storm. The convenience of its technology coupled with the relatively simple process through which it is now created, ensures that RFID will continue to make its presence known. Although there are still obstacles to be overcome, mainly concerns from advocates of personal privacy, RFID is becoming an integral part of this growing digital world.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX 1

## A. TIMELINE OF DOD'S JOINT TOTAL ASSET VISIBILITY DIRECTIVE

April 1992 - Original DoD TAV Plan Published

March 1994 - DUSD(L) TAV Conference

(1st Savi Contract awarded)

September 1994 - DoD TAV Joint Task Force formed

1995 - Implementation Plan Published - Staffed with Combatant Commanders and Services

April 1995 - Army Appointed Executive Agent

June 1995 - JTAV Office Established

January 1996 - JTAV Office Staffed with 20 Service / Agency / Component Representatives

(2nd Savi Contract awarded)

February 1996 - JTAV-IT Deployed to EUCOM

November 1996 - JTAV-IT Deployed to CENTCOM

May 1997 - JTAV-IT Deployed to ACOM

July 1997 - Functional Requirements Document Published

December 1997 - JTAV-IT Web Version Released

March 1998 - JTAV-IT Deployed to PACOM

June 1998 - Initial Demo of Objective Architecture

June 1998 - DLA Appointed Executive Agent

August 1998 - Phase I National Level Ammunition Capability Fielded

September 1998 - Medical Shared Data Server Operational

October 1998 - JTAV-IT Deployed to SOUTHCOM

October 1998 - JTAV-IT Deployed to SOCOM

January 1999 - JTAV Strategic Plan Published

January 1999 - Start Beta Test of Objective Architecture

January 1999 - Phase II National Level Ammunition Capability Fielded

Oct 01-Sep 05 - JTAV Sustainment

-2002 – AIT/RFID mandated for all U.S. military branches

-2003 - 3rd Savi contract awarded

-July 2004 - DoD Sets final standards for its RFID Policy

Savi's Timeline

1989 - Savi founded by Rob Reis.

1990-91 - DARPA grant to research how automatic identification and data collection technologies and Internet can be deployed for logistics

1991 - Savi awarded three Navy SBIRs totaling $2.5 million

1993 – Retrograde shipments to Europe

1994 – First DoD RFID procurement contract awarded to build

real-time wireless monitoring (Savi Technology) $70 million dollars

1994-2001 – Somalia, Haiti, Bosnia, Afghanistan (“AIT enabled a 30% reduction in logistics assets, such as containers for the Bosnia operation.” ***DOD Study on Bosnia logistics operations***

1996 – ***GAO report*** states that DoD could have saved $2 Billion in costs if AIT/RFID were used in Desert Storm (“Just-in-Case Logistics”)

1996 – Navy: Fleet Industrial Support Center - Guantanamo Bay, Cuba outfitted with RFID network

1997 - Second Contract awarded to Savi - $111 million

1997-present – Pacific Theater Sustainment

1997 - present–FORSCOM Power Projection Platform

2002 - Savi partners with over 70 companies to form the Smart and Secure Tradelanes initiative. The initiative manages over 75% of worldwide cargo shipments and trade

2003 – Third DOD RFID procurement contract awarded $90million

2003 - Savi Awarded contract to become the primary supplier of RFID Solutions to the United Kingdom's Ministry of Defense

2003 - Savi is awarded a contract to develop an RFID network for NATO forces as part of a pilot program for force integration in Afghanistan

2004 - Savi is awarded a defense contract with the Danish Military. Savi is now the primary provider of RFID to the military's of the US, UK, and NATO.

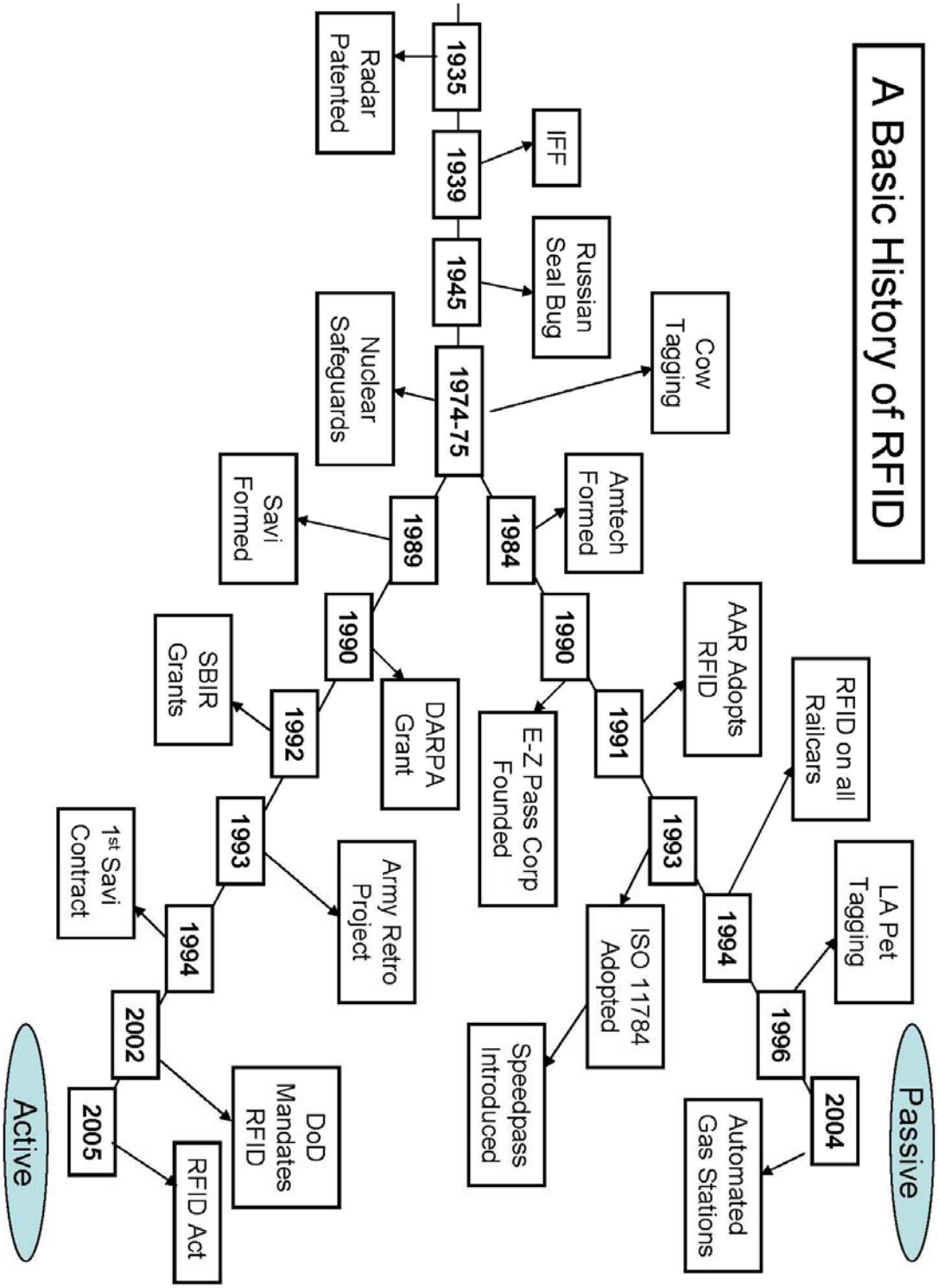
2003 – RFID used in support of Operation Enduring Freedom & Operation Iraqi Freedom

2005 - Savi announces new technology integrating parts from Savi, Zebra and Symbol to meet the DoD UID requirements. RFID-ACT (RFID - Assured Compliance today)

2005 - Savi is the worldwide leader in real-time supply chain asset management and security. Tom Ridge, former Director of Homeland Security, joins the board of directors.

# APPENDIX 2

## A. A BASIC HISTORY OF RFID



THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


1. Jackson, R.J. "Radio Frequency Identification (RFID)," a white paper. 17 December 2004. [http://home.att.net/~randall.j.jackson/rfid.htm].

2. Murray Associates. "The Great Seal Bug Story." [http://www.spybusters.com/Great_Seal_Bug.html]. April 2005.

3. Halliday, Steve. "The RFID facts." [http://www.hightechaid.com/tech/rfid/rfid_facts.htm]. April 2005.

4. Gilmore, Dan. "As the RFID World Turns." [http://rfidinc.com/turns.html]. April 2005

5. Eagleson, Jim. "RFID: The Early Years 1980-1990." [http://members.surfbest.net/eaglesnest/rfidhist.htm]. March 2005.

6. Wikipedia. "RFID." [http://en.wikipedia.org/wiki/RFID] March 2005.

7. Shimek, Cary. "Harnessing the Honeybee." *Research View*. Spring 2004. [http://www.unt.edu/urelations/rview/spring04/honey.htm]. April 2005.

8. Sandia National Laboratories. "Sandia, University of Montana researchers try training bees to find buried landmines." [http://www.sandia.gov/media/minebees.htm]. April 2005.

9. Wikipedia. "LIDAR." [http://en.wikipedia.org/wiki/Lidar. April 2005].

10. Weideman, Paul. "A Short History of Los Alamos." [http://www.freenewmexican.com/artsfeatures/102.html]. April 2005.

11. Goebel, Greg. "The British Invention of Radar." [http://www.vectorsite.net/ttwiz1.html]. April 2005.

12. Liu, D. and others. “Laser Direct-Write Technology and Its Low Processing Temperature Low Cost Applications.” *Advancing Microelectronics*. March/April. Volume 29. No 2.

13. Gay, Paul. “Advanced Manufacturing – Direct Writing.” [http://www.dti.gov.uk/technologyprogramme/pdfs/direct_writing.pdf]. April 2005.

14. Landt, Jerry. “Shrouds of Time: The history of RFID.” AIM Global. 01 October 2001. [http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf]. March 2005.

15. DeGaspari, John. “Minding Your Beeswax.” *Mechanical Engineering Magazine*. Feb 2005. [http://www.memagazine.org/backissues/feb05/departments/tech_focus/techfocus2.html].

16. Chrissey, D.B. and others. “The Future of Direct Writing in Electronics.” [http://www.circuitree.com/CDA/ArticleInformation/coverstory/BNPCoverStoryItem/0,2135,142466,00.html]. April 2005.

17. Bromenshenk, J.J. and others. “Can Honey Bees Assist in Area Reduction and Landmine Detection.” *Journal of Mine Action*. Issue 7.3. December 2003. [http://maic.jmu.edu/journal/7.3/focus/bromenshenk/bromenshenk.htm]. April 2005.

18. Interview between R. Acevedo. LCDR, USN. Naval Postgraduate School, and Mr. Ron Gilbert, 27 Mar 2005.

19. Telephone conversation between LCDR R. Acevedo. LCDR, USN. Naval Postgraduate School, and Mr. Jerry Landt, 28 Mar 2005.

20. Telephone conversation between LCDR R. Acevedo. LCDR, USN. Naval Postgraduate School, and Mr. Jerry Bromenshenk, 16 April 2005.

21. Diamond, Jared. *Guns, Germs & Steel*, 1st. pp 1-42, 240-260, W.W. Norton & Company, April 1997

22. Interview between R. Cooper, Lieutenant, USNR and Vic Verma, President and CEO, Savi Technology, 02 June 2005.

23. Lee, H.L., Whang, S., Higher Supply Chain Security with Lower Cost; Lessons from Total Quality Management, Stanford University, Stanford, CA, July 2003.

24. Diamond, Jared. "The Curse of QWERTY." [http://www.tks.buffalo.edu/~scomings/Sgc/dv-art.html]. April 1997.

25. Davis, H.C., Jones, S.R., "RFID Technology: Is the capability a Boon or Burden for the DoD?" Air Force Logistics Management Agency, 2004 Logistics Dimensions, v. 1, pp. 229-232, August 2004.

26. Hill, Daniel. US Small Business Administration, Public Testimony, pp. 3, 17 June 1999.

27. David, Paul. "Clio and the economics of QWERTY" [http://wwwpub.utdallas.edu/~liebowit/knowledge_goods/david1985aer.htm] 1985.

28. RFID News. "Savi Debuts DoD Solution." [http://www.rfidnews.org/news/2004/09/30/savi-debuts-dod-solution/]. September 2004.

29. ZDnet. "US Military expands radio-wave tracking." [http://news.zdnet.com/2100-1009_22-984391.html] February 2003.

30. MobileInfo. "AIDC Technology" [http://www.mobileinfo.com/AIDC/RFID.htm] December 2001.

31. Department of Defense. "SBIR/STTR Program Successes" [http://www.acq.osd.mil/sadbu/sbir/success/]. April 2005

32. RFID Journal. "Savi wins $90M RFID Contract." [http://rfidjournal.com/article/articlereview/296/1/1/]. February 2003.

33. RFID Journal. "Danish Defense contracts with Savi." [http://rfidjournal.com/article/articlereview/1246/1/14/]. November 2004.

34. National Defense Magazine. "Electronic Identification Tags Aid Logistics." [http//www.nationaldefensemagazine.org/issues/2003/Aug/Electronic_Identification.htm]. August 2003.

35. RFID Update. "Tom Ridge joins Savi Technology Board of Directors." [http://www.rfidupdate.com/articles/?id=844] April 2005.

36. RFID Journal. "Gillette to Buy 500 Million EPC Tags." [http://rfidjournal.com/article/article/view/115/1/1/]. November 2002.

37. Newsmax. "Li Ka-Shing Seeks US Contract." [http://www.newsmax.com/archives/articles/2002/8/5/181935.shtml]. August 2002.

38. Supply and Demand Chain Executive. "New RFID System from Savi." [http://www.sdcexec.com/article_arch.asp?article_id=4715]. October 2003.

39. Department of Defense Small Business Innovation Research. "A Dod SBIR Success Story." [http://www.dodsbir.com/Materials/SuccessStories/Savi.htm]. April 2005

40. Government Security. "Managing assets physical & information with the help of technology." [http://govtsecurity.com/mag/managing_assets_physical/]. December 2004.

41. Military Information Technology. "RFID: 'In the Box' Visibility" [http://www.military-information-technology.com/article.cfm?DocID=168]. August 2003.

42. Business Journal. "Savi receives $111M to track Military Supplies." [http://www.bizjournals.com/sanjose/stories/1997/08/25/newscolumn5.html?page=1]. August 1997.

43. Logistics Today. "Savi Technology Awarded $90 Million US Military Contract." [http://logisticstoday.com/sNO/4941/LT/displayStory.asp]. February 2003.

44. Savi Technology. "Savi Technology Unveils Dod Supply Chain Rfid Solution Featuring Industry-Leading Components From Symbol And Zebra." [http://www.savi.com/news/2005/2005.02.09.shtml]. February 2005.

45. Savi Technology. "Savi Technology And Comtech Telecommunications Combine Rfid, Gps And Satellite Communications To Continuously Manage Transport Vehicles And Their Cargo." [http://www.savi.com/news/2005/2005.03.15.shtml]. March 2005.

46. Savi Technology. "Savi Technology And Samsys Technologies Integrate Rfid Solution To Bolster Security At U.S. Army Ammo Depots." [http://www.savi.com/news/2004/2004.04.07.shtml]. April 2004.

47. Savi Technology. "Nato Signs Contract With Savi Technology For Wireless Logistics Pilot Project Between Europe And The Middle East." [http://www.savi.com/news/2004/2004.03.24.shtml]. March 2004.

48. Savi Technology. "U.S. and China Drive Global Momentum for Active RFID Band Used by Savi Technology for Real-Time Supply Chain Visibility." [http://www.savi.com/news/2004/2004.06.09.shtml]. June 2004.

49. Savi Technology. "Company History." [http://www.savi.com/company/ov.fact.shtml]. May 2005.

50. Savi Technology. "'Smart Box' Rfid Technology Urged By U.S. Customs For Security Also Provides Economic Value For Global Shippers - A.T. Kearney." [http://www.savi.com/news/2005/2005.01.30.shtml]. January 2005.

51. Savi Technology. "Savi Sentinel ST-646." [http://www.savi.com/products/ds.sentinel.pdf]. May 2005

52. Army Quartermaster Professional Bulletin. "RFID Initiatives - The Race against Time and Technology." [http://www.quartermaster.army.mil/Professional_Bulletin/2004/Summer04/RFID_Initiatives_The_Race_Against_Time_and_Technology.htm]. July 2004.

53. Wykle, K.R., Powerpoint Presentation, RFID Journal Live, [www.rfidjournal.com/live/Wykle_Transportation.pdf]. June 2003

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California